MARK A. CHAVEZ (Bar No. 90858)
mark@chavezgertler.com
Chavez & Gertler LLP
42 Miller Ave.
Mill Valley, CA 94941
(415) 381-5599 (telephone)

MARC ROTENBERG[1] (to be admitted pro hac vice)
rotenberg@epic.org
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Amicus Curiae
the Electronic Privacy Information Center

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE GOOGLE STREET VIEW ELECTRONIC COMMUNICATIONS LITIGATION This Pleading Relates To: ALL CASES	Case No. 5:10-CV-00672-JW **BRIEF FOR *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF PLAINTIFFS**

[1] Mr. Rotenberg is barred in the District of Columbia, the Commonwealth of Massachusetts, the U.S. Supreme Court, and several federal Circuits Courts. He participated in the development and drafting of the ECPA of 1986. EPIC Appellate Advocacy Fellow Conor Kennedy contributed to the preparation of this brief.

The Electronic Privacy Information Center ("EPIC") respectfully files this *amicus curiae* brief in response to this Court's order request for supplemental briefing (Dkt. No. 73).

Interest of Amicus Curiae

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.

EPIC has participated as *amicus curiae* in numerous cases that concern emerging privacy issues before the Supreme Court and other courts, including *IMS Health Inc. v. Sorrell*, 630 F.3d 263 (2d Cir. Vt., 2010) *cert. granted, Sorrell v. IMS Health*, 79 U.S.L.W. 3397 (U.S. Jan. 11, 2011) (No. 10-779), *Tolentino v. New York*, 2011 U.S. LEXIS 2593 (U.S. Mar. 29, 2011); *NASA v. Nelson,* 131 S. Ct. 746 (2011); *Doe v. Reed,* 130 S. Ct. 2811 (2010); *Quon v. City of Ontario,* 130 S. Ct. 2619 (2010); *Flores-Figueroa v. United States*, 129 S. Ct. 1886 (2009); Herring v. United States, 555 U.S. 135 (2009); *Crawford v. Marion County Election Board,* 553 U.S. Ct. 181 (2008); *Hiibel v. Sixth Judicial Circuit of Nevada,* 542 U.S. 177 (2004); *Doe v. Chao,* 540 U.S. 614 (2003); *Smith v. Doe, 538* U.S. 84 (2003); *Department of Justice v. City of Chicago, 537* U.S. 1229 (2003); *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton,* 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000).

Summary

The Electronic Communications Privacy Act ("ECPA") constitutes a set of amendments to the federal wiretap law of 1968 that seek to update and expand privacy protections for modern communications technologies. As such, the law should be understood to establish privacy safeguards for users of new communications services. "The paramount purpose of the Wiretap Act is to protect effectively the privacy of

communications." *In re Pharmatrak, Inc.,* 329 F.3d 9, 18 (1st Cir. 2003). Exemptions set out in the Act address specific circumstances identified by lawmakers where it was either impractical or undesirable to prohibit the interception of private communications at a particular moment in time.

The term "configured" in the evaluation of those communications that are "publicly accessible" reflects an intent by Congress to create a presumption in favor of confidentiality except in those circumstances where the user has knowingly chosen to broadcast communications to the general public. While a handful of operators of home networks may choose to configure their wireless devices to enable public access to the Internet, the vast majority of operators of such home devices have not done so. Indeed, it is widely know that to configure devices in this way makes wireless networks subject to attack. The straightforward reading of the purpose of the Act is to treat the interception of such communications as unlawful.

(a) "Radio Communications" are Protected From Intercept Under ECPA where the User of a Communications Device Does Not Intend to Broadcast Communications to the General Public

In 1986, the drafters of the amendments to the federal wiretap law exempted a very specific set of "radio communications" from the general provisions protecting "electronic communications" against third party interception. 18 U.S.C. §§ 2510(16)(A)-(E); 2511(2)(g)(i), (ii). Congress's decision to exempt radio interception reflected the fact that public-interest amateur hobbyists operated on the radio portion of the electromagnetic spectrum at the time of ECPA's passage. As such, Congress sought to protect the broadcast transmission of radio operators from the penalties established by the ECPA. As the House Committee Report noted:

> The Committee considered listing all the existing radio services which are exempt from the bar on interceptions, but rejected that approach because it would been cumbersome, possibly redundant, and would have had a built-in obsolescence . . . . Therefore instead of listing all of these services the Committee listed some of the

> more common radio services. In addition, the bill includes a "generic" exception relating to radio services which are "readily accessible to the general public."

H.R. Rep. No. 99-647 at 42 (1986). But the exemption was narrow and intended to apply to amateur radio operators only. Congress noted that that FCC Rules and Regulations governing amateur radio services even "prohibit[ed] business communications" and other commercial uses of the spectrum. Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary, 99th Cong., 1st & 2d Sess. 151.

The House Committee Report accompanying the bill to the floor declared that "[a]mateur radio communications . . . . are certainly not those to which this legislation is aimed," predominantly because "[a]mateurs have legitimate reason to monitor frequencies outside the amateur bands." H.R. Rep. No. 99-647 at 42 (1986). Congress called upon the largest membership associations of amateur radio enthusiasts in the country to supply testimony to the Subcommittee that drafted ECPA. Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary, 99th Cong., 1st & 2d Sess. 146-209 (1985) (statements of Larry E. Price, President, American Radio Relay League and Richard T. Colgan, Executive Secretary, Ass'n of N. Am. Radio Clubs). In hearings, both groups testified that radio scanning practices uniquely enabled their amateur operators to provide emergency communications for distress calls where other facilities are "destroyed or overtaxed." Id. at 168. Amateur radio operators also explained the significance of their role in "phone patching" communications between wounded American military personnel and hospital ships or family members back home. *Id.* at 153. The House Committee Report reflected these interests:

> Many amateurs, for instance, are enrolled in the Military Affiliate Radio System and the Civil Air Patrol . . . Some 30,000 amateurs are part of Skywarn, a system

> operated by the National Weather Service for tracking and warning of severe weather conditions.

H.R. Rep. No. 99-647 at 42. *See also*, 47 C.F.R. § 97.1 (1988) (discussing benefits of amateur radio operations).

Commentators have also noted that the exception for amateur radio operators would not apply more broadly to other activities. *See, e.g.*, Fred Jay Meyer, *Don't Touch That Dial: Radio Listening Under the Electronic Communications Privacy Act of 1986*, 63 N.Y.U. L. Rev. 416, 423-24 (1988) ("Those who conduct electronic surveillance, utilizing radio receivers and other electronic equipment to seek out, intercept, and monitor targeted electronic communications, are distinct from hobbyists and other casual radio listeners.")

Regarding the statutory carve-out for unscrambled and unencrypted radio messages, 18 U.S.C. § 2510(16)(A), the provision does not apply to private Wi-Fi networks. The provision was first proposed by the Association of North American Radio Clubs, Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary, 99th Cong., 1st & 2d Sess. at 169-70, and was designed to permit amateur radio wave operators to exempt their efforts to listen to mobile radio services that "do not take even minimal precautions against interception of their transmissions." Id. at 168.

Radio scanners are a niche community of sophisticated users who have understood the widespread availability of receivers that scan amateur radio signals for local emergency communications. Amongst experts, encryption was a proxy for the transmitter's regard for the protection of its communications: "a test of whether the system provider or user expects . . . privacy." *Id.* But for a typical user of a device that had a broadcast capability, the distinction would not be meaningful as the general user would not have the training or the ability to enable or disable this functionality.

The Act anticipated this problem by including the word "configured" in the consideration of whether or not the transmission was "publicly accessible." The aim was to ensure that the operators of devices would make a knowing decision to enable access to broadcast communications.

(b) Typical Wireless Home Networks Enable Communications Among Devices within the Home and are Not Configured for Public Access.

Many people establish home wireless networks, also called "Wireless Local Area Networks" ("WLAN"), *to enable communications between devices within the home*. For example, a WLAN might connect a desktop computer in an office with a laptop in the kitchen and a media device in the living room. The home network might provide a common printer available to each of the devices, as well as Internet access so that each device within the home can share a single subscription with an Internet Service Provider ("ISP"). The use of a wireless network device in this configuration is both less expensive and more flexible than a hardwired Local Area Network ("LAN"), which would require fixed cabling and additional switching. The functionality of wireless networks is directed toward those within the home who take advantage of these shared services.

WLANs typically have a limited transmission range. Unlike broadcast technologies, WLAN are not intended to be accessible to the general public. However, there are separate categories of devices that are designed to broadcast to a wider region and that may operate as an alternative to cellular networks. These devices include Wireless Metropolitan Area Networks ("WMAN"), which are described by the IEEE 802.16 standard and includes WiMAX, and Wireless Wide Area Networks ("WWAN") networks that "cover large outdoor areas." *See generally*, Wikipedia, "Wireless networks." (WiMAX is viewed as a possible replacement for cellular phone technologies such as GSM and CDMA precisely because it can cover a broad geographic region.)

There is also Long Range Wi-Fi, also known as "Wi-Fi over Long Distance" ("WiLD") that is intended to provided long distance wireless access. "The (TIER) project at University of California at Berkeley, in collaboration with Intel, utilizes a modified Wi-Fi setup to create long-distance point-to-point links for several of its projects in the developing world." Wikipedia, "Long Range Wi-Fi," http://en.wikipedia.org/wiki/Long-range_Wi-Fi.

Within this taxonomy, a WLAN to enable communications among devices within a home would not be considered a broadcast technique. Its purpose is to establish a *Local* Area Network, accessible to an identifiable set of users.

A wireless Home network should also be distinguished from a "Wi-Fi Hotspot" that is configured so as to enable public access to the Internet. Many commercial businesses, particularly those that are trying to generate walk-in traffic such as coffee shops, might choose to create a Wi-Fi hotspot to attract customers. By way of example, Starbucks has an estimated 7,000 Wi-Fi hotspots in the United States. The company recently decided to make the hotspots freely available and advertised this fact to promote business. Starbucks, "Free Wi-Fi for Everyone. Now at Starbucks," http://www.starbucks.com/coffeehouse/wireless-internet/. And Starbucks took the necessary steps to ensure that the devices were accessible to the public. Municipalities might also choose to establish free public Wi-Fi access points. Seattle is among the cities leading an effort to promote Internet access through "Seattle Wi-Fi." As the city explains, "The goals of the City's Wi-Fi pilot project are: to attract more customers to local business districts, support small businesses, encourage the use of public parks and facilities, and enable more citizens to access City services online." Seattle.gov, "Wi-Fi in Seattle – Technology – Community – Living in Seattle – Seattle.gov," http://www.seattle.gov/html/citizen/wifi.htm

Wi-Fi Hotspots serve an important purpose, *when they are configured by the operator,* to enable Internet access. But it would be very unusual for the operator of a residential network to configure a device in this way. Not only would the home user obtain none of the typical benefits for public Wi-Fi Hotspot – increased interest in and traffic to the physical location – the user would take on the additional risk that the network could be hijacked and used for spam, fishing, and other illegal activities.

(c) Under ECPA, Cellular Communications were First Protected by Warnings to the Consumer, and then Further Amendments to Act

In 1986, Congress determined that cordless telephones would not be protected in the amendments to the Wiretap Act because "those conversations are often picked up unintentionally on FM radio receivers." Mary Thornton, *House Panel Votes to Modernize Curbs on Electronic Eavesdropping,* Wash. Post, May 15, 1986, at A13. However, Congress also sought to provide adequate warnings to consumers about the risk of using wireless devices that lacked legal protection. It required a prominent warning label: "PRIVACY OF COMMUNICATIONS MAY NOT BE ENSURED WHEN USING THIS PHONE." H.R. Rep. No. 99-647 at 43.

No similar warnings are provided to residential users of wireless network devices.

In 1994, Congress provided the same statutory protections to radio communications services as it did to other electronic communications. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, § 202, 108 Stat. 4279, 18 U.S.C. § 2510. This decision followed, in part, from the 1991 Privacy and Technology Task Force Report, which found that:

> [t]he cordless phone, far from being a novelty item used only at 'poolside,' has become ubiquitous . . . More and more communications are being carried out by people [using cordless phones] in private, in their homes and offices, with an expectation that such calls are just like any other phone call.

See H.R. Rep. No. 103-827, at 19 (1994).

Conclusion

The Electronic Communications Privacy Act reflects an intent by Congress to update privacy protections for electronic communications in response to technological innovation. Congress understood that there would be a category of broadcast communications, generally accessible to the public, that should fall outside the reach of ECPA. But Congress sought to keep that exception narrow and to make clear that the operator of the service, through the configuration of the device, intend that the communications be public. It is not reasonable, sensible, or consistent with the intent of ECPA to imagine that the operator of a wireless home network would intend that the network be accessible to the general public.

Dated: April 11, 2011

Respectfully submitted,

/s/ *Mark A. Chavez*

MARK A. CHAVEZ (Bar No. 90858)
Chavez & Gertler LLP
42 Miller Ave.
Mill Valley, CA 94941
(415) 381-5599 (telephone)

/s/ Marc Rotenberg

MARC ROTENBERG[2] (to be admitted *pro hac vice*)
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)
efiling@epic.org (email)
Attorneys for the Amicus Curiae the Electronic Privacy Information Center

[2] Mr. Rotenberg is barred in the District of Columbia, the Commonwealth of Massachusetts, the U.S. Supreme Court, and several federal Circuits Courts.